WHAT IS CLAIMED IS:

1. A system for manipulating a computer file and/or program comprising:

a serving device having access to a computer file and/or program which is unencrypted and which can encrypt the unencrypted computer file and/or program to become an encrypted computer file and/or program and transfer it;

a connector connected to the serving device on which the encrypted computer file and/or program travels and to which the serving device transfers the encrypted computer file and/or program; and

a client device which receives the encrypted computer file and/or program and decrypts the encrypted computer file and/or program back to the unencrypted computer file and/or program, said client device not allowing intervention to the encrypted computer file and/or program during a time when the encrypted computer and/or file program is received, said serving device separate, apart and distinct from the client device.

2. A system as described in Claim 1 wherein said server device assigns permissions and/or rights to the unencrypted computer file and/or program which identifies what the client device can do with the unencrypted or encrypted computer file

and/or program after the client device has received the encrypted computer file and/or program or after the client device has decrypted the encrypted computer file and/or program back to the unencrypted computer file and/or program.

3. A system as described in Claim 2 wherein said server device encrypts the permissions and/or rights and transfers them to the client device through the connector, said client device decrypts the unencrypted permissions and/or rights.

4. A system as described in Claim 3 wherein the serving device includes controlling server software and/or firmware which causes the encryption of the unencrypted computer file and/or program and the permissions and/or rights and instructs the client device to temporarily suspend user intervention when the client device receives the encrypted computer file and/or program and the encrypted permissions and/or rights.

5. A system as described in Claim 4 wherein the client device includes controlling client software and/or firmware which causes the decryption of the encrypted computer file and/or program.

6. A system as described in Claim 5 wherein the client device has a mechanism for requesting the unencrypted computer file and/or program from the server device.

7. A system as described in Claim 6 wherein the controlling client software and/or firmware causes the encryption of the unencrypted computer file and/or program and the permissions and/or rights for storage.

8. A system as described in Claim 7 wherein the client device has an operating system and the controller client software and/or firmware instructs the operating system to reestablish user intervention at a desired time.

9. A system as described in Claim 8 wherein the server device has a server public key infrastructure which encrypts using encrypted communication protocols the permissions and/or rights and the unencrypted computer file and/or program.

10. A system as described in Claim 9 wherein the client device has a client public key infrastructure which decrypts from transmission the permissions and/or rights and encrypted computer file and/or program using encrypted communication protocols.

11. A system as described in Claim 10 wherein the client device includes an encrypting file system which encrypts the unencrypted computer file and/or program and the permissions and/or rights and allows for the manual selection of the unencrypted computer file and/or program for encryption or decryption.

12. A system as described in Claim 11 wherein the client public key infrastructure has an encryption and/or decryption key and the encrypting file system uses the encryption and/or decryption key utilized by the client public key infrastructure.

13. A system as described in Claim 12 including a next client device connected to the client device through the connector.

14. A system as described in Claim 13 wherein the controlling client software and/or firmware moves or copies the encrypted computer file and/or program to the next client device through the second connector, said client device having a controlling next client software and/or firmware which decrypts the received encrypted computer file and/or program and the encrypted permissions and/or rights and temporarily suspends user intervention of the next client device while the encrypted computer file and/or program is received by the next client device.

15. A system as described in Claim 14 wherein the connector includes a communication link, the server device includes a transmitter connected to the communication link for transferring the encrypted computer file and/or program and unencrypted permissions and/or rights to the communication link, and the client device includes a receiver connected to the communication link which receives the encrypted computer file and/or program and the encrypted permissions and/or rights from the communication link.

16. A system as described in Claim 15 wherein the first and second connectors are part of the Internet or other communication network.

17. A method for manipulating a computer file and/or program comprising the steps of:

suspending intervention by a user at a client device of the client device;

encrypting an unencrypted computer file and/or program at the server device to form an encrypted computer file and/or program;

transferring the encrypted computer file and/or program to the client device along a connector connected to the client device and the server device; and

reestablishing the intervention of the client device by the user.

18. A method as described in Claim 17 including before the transferring step, there is the step of encrypting permissions and/or rights of the unencrypted computer file and/or program and transferring the encrypted permission and/or rights to the client device along the connector from the server device.

19. A method as described in Claim 18 including before the encrypting the unencrypted computer file and/or program step, there is the step of requesting by the client device the unencrypted computer file and/or program of the server device.

20. A method as described in Claim 19 including after the requesting step, there is the step of copying a primary unencrypted computer file and/or program to form the unencrypted computer file and/or program.

21. A method as described in Claim 20 including before the reestablishing step, there is the step of decrypting the encrypted computer file and/or program back to the unencrypted computer file and/or program at the client device.

22. A method as described in Claim 21 including after the decrypting step, there are the steps of encrypting the unencrypted computer file and/or program and permissions and/or rights at the client device and storing the encrypted computer program and/or file and the encrypted permissions and/or rights in the client device.

23. A method as described in Claim 22 including after the storing step, there is the step of transferring the encrypted computer file and/or program to a next client device connected to the client device by a second connector.